

THE DIRECTOR OF CENTRAL INTELLIGENCE

WASHINGTON, D. C. 20505

IC 75-2525

Admiral George W. Anderson, Jr., USN (Ret.)
Chairman, President's Foreign
Intelligence Advisory Board
The White House
Washington, D. C. 20500

Dear Admiral:

I am writing now concerning heightened anxiety in the community and in my own mind over leaks to the press of sensitive intelligence data. I want to share with you and the Board my present appreciation of the problem and to seek your advice and recommendations.

As you well know, unauthorized public disclosures of intelligence information have occurred frequently in recent years. A more important consideration, however, is that press revelations have come increasingly to include explicit and generally accurate details about the methods we use to obtain and exploit sensitive information. In the past year we have witnessed a further upswing in the number and severity of damaging intelligence leaks--a situation I can only describe as a virtual hemorrhaging of the security control system. And it seems clear that journalists are not just being briefed orally: they are now being given direct access to highly classified documents.

Recently I had my staff take a fresh look at the problem to see if there were not some as yet untried way--within the means at my disposal--to halt and reverse this trend. Although I did this with a sense of having been through the exercise many times before, it was still essential to try again, not only because of the damage individual leaks can cause to our long-term capabilities, but because the present situation also generates widespread discouragement and frustration--even cynicism--within the ranks of the intelligence community itself. This has the potential for lowering security discipline even more.

In the past, expressions of serious concern over intelligence leaks have been voiced by successive Presidents and their department heads following a particularly grave leak or a series of damaging leaks. My predecessors and I have responded largely by trying to improve document and personnel security practices, issuing guidelines to Government departments on procedures for sanitizing the intelligence to be used by administration officials for public purposes, and carrying out investigations of the more flagrant and damaging leaks. These are all necessary steps, but clearly they have been insufficient, and simply repeating them will-- in my view--prove no more effective now than in the past.

To tackle this problem constructively, I believe we must be quite frank. We have, I believe, focused so intently on the conditions that make intelligence leaks possible that we have slighted consideration of the climate of opinion in and out of Government that actually encourages them.

The widespread public dissemination of classified intelligence information does not represent a direct breakdown of the elaborate system of classification, document controls, personnel security checks, indoctrination practices, and application of the "need-to-know" principle which we use to minimize the risks of exposing sensitive data to the many persons who must work on and use them. The overwhelming number of such disclosures come not from the rank and file of analysts and drafters who were privy to the materials within the intelligence community. Rather, most represent deliberate disclosures by senior or relatively senior officials with an unquestionable "need to know"--most of them outside the intelligence community--who evidently believe that the public benefits of disclosing the information far outweigh the damage or risks involved.

Many disclosures identifiably represent a calculated "official" judgment at departmental level that previously classified material--say, on ICBM deployments--could be properly declassified and released. While other disclosures are usually less easy to pinpoint as to source, most of them appear designed to promote the programs, policies, or interests of particular elements within the Government--or to rebut those of others--as part of the continuing process in which national security policies are hammered out. Relatively few can be readily construed as the disclosures of a disgruntled or venal underling.

Most of the "official" disclosures noted above, and quite a few of the others, have probably involved no serious threat to intelligence sources and methods. A good deal of the intelligence we collect, notably in the area of overhead reconnaissance, is less sensitive than it once was. What is increasingly disregarded, however, is that there remain many sensitive areas of information and analysis, often identifiable as such only by intelligence specialists, where disclosure could be highly detrimental. Unfortunately, however, there is no established Government-wide procedure for determining who can declassify intelligence information and for assuring that it is properly sanitized before release, and there is a marked reluctance within the responsible Government departments to pursue investigations of potentially damaging disclosures that point toward relatively senior levels of officials. Meanwhile, the increasing frequency of disclosures of classified intelligence information--whether "official" or not--encourages the growth of a permissive atmosphere in which it seems that almost anything goes.

I see the press as largely an instrument in this process--not a direct cause of it. While there are examples of what I consider gratuitous and irresponsible exposure of sensitive data on the part of individual journalists, most of these persons see themselves as conforming to a widespread and generally accepted standard. Much of what they report has been made available to them by presumably responsible officials who clearly intended to have the information made public. And in the present atmosphere of disclosures, small wonder that many of the more energetic reporters feel that any information they can dig out is fair game.

In sum, I believe our basic problem is with an increasingly prevalent state of mind among many senior officials in the Executive Branch, among members of the press, and among many in the Congress. This involves a line of reasoning containing one or more of the following elements:

The democratic process requires informed open debate, and if the price of that is an occasional risk to intelligence, it must be paid.

The intelligence community has been overprotective and unnecessarily secretive about sources and methods everyone knows it employs. Despite frequent alarms about the alleged damage caused by past disclosures, the US still has a highly effective system for collecting intelligence information. The problem, if any, is rather with how effectively it uses the material.

The "leakage" issue is at least partially a red herring, because every administration so far has selectively released intelligence information to its own advantage. There are complaints about "leaks" only when information which doesn't support the official view gets out.

That line of reasoning cannot lightly be dismissed: there is in fact much truth in it. The price of a free society must be paid if we are to retain the democratic process. The intelligence community probably has been overinclined to classify everything as a matter of course, and often overly shrill in claiming irreparable damage to its sources and methods when leaks have occurred. And there is some validity to the argument that the Government has at times appeared to follow a double standard in evaluating damage of intelligence disclosures and placing blame according to who makes them and whose policies they support.

Unfortunately, when the issue is posed in these terms the wrong dichotomy is emphasized. The proper question is not the public need to know versus the parochial interests of the intelligence services and the administration for self-protection. The issue is rather between the short-term and long-term interests of us all. In other words, a sound and defensible balance is needed between the contemporary domestic imperatives of an open society and the preservation of an ability in the future to detect dangers to that society that originate from abroad.

There are somewhat parallel dilemmas in other areas of Government which I have often referred to. For example, our military forces must be responsive to civilian control, but the public does not demand that detailed war plans be published. Our judicial system must meet the public's standards of justice, but

grand jury proceedings are not conducted in the open. It is even necessary for the Congress to conduct some of its business in executive session, while remaining accountable to the voters for the legislation it passes. What we no longer can count on is a general public understanding and acceptance of the need for similar trade-offs between openness and confidentiality in the field of foreign intelligence.

To deal with the problem of protecting vital sources and methods against unwarranted disclosure, there is a clear need to consider significant departures from the limited approaches that have been taken in the past. As I see it, there are several areas that call for careful and simultaneous attention:

Continued efforts within the intelligence community are needed to limit the opportunity for inadvertent or intended (but unauthorized) disclosures of classified information when the disclosures are made by persons in the intelligence services, and to facilitate successful investigation and application of penalties. A number of activities are under way within the USIB arena to study this problem and to make such changes as are necessary in the classification and compartmentation system and in controlling the dissemination of sensitive data.

There is also a need to develop more effective controls and sanctions relating to disclosures of foreign intelligence information by officials outside the intelligence services of Government departments. No adequate procedures or common standards exist for determining accountability for press disclosures or for guiding the preparation of authorized texts for public disclosures and for reporting them. This would require action by USIB in concert with several other departments of Government.

Ways need to be devised to discourage and if necessary penalize unauthorized disclosures by advocates of particular programs or policies within the Government and by contractors with access to intelligence data. The availability of judicial sanctions would be helpful in this regard--and I have proposed legislation to that end--but a greater degree of organizational

and ultimately self-imposed discipline by senior officials within Government is equally essential. This is probably the most difficult of all objectives to achieve. It lies almost wholly outside the intelligence community's ability to do more than seek to persuade, and it involves the delicate question of how each administration wishes to deal with adversary procedures within its own ranks. Its achievement would clearly require a significant change in attitude not only by the officials directly involved but ultimately by key elements in the Congress and the press and the public with whom they must deal. But I feel certain that the lack of such discipline has come to be a central weakness in our foreign intelligence security control system, and I would be derelict in not forthrightly saying so.

Finally, the intelligence community needs itself to re-examine its traditional classification standards and practices, with a view to being more forthcoming in making public those intelligence findings and materials whose disclosure would not create security problems or diplomatic difficulties or otherwise damage the national interest. Only if we are seen to be reasonable in such matters can we expect full acceptance of our demands for continued protection of data which remains sensitive. In this, a more careful distinction must be made among what I have termed good secrets, bad secrets, and non-secrets. I am taking some initiatives in this area but will wish to obtain the views of others--including the PFIAB--as well.

The situation we face is serious--and getting worse. It is almost overwhelming in its complexity and resistance to solution. The attitudinal factors which encourage disclosures are the dominant elements of my concern right now, because they feed and nourish the trend. And yet there is little I alone can do on that central problem. I have outlined some areas that need attention, and request your early consideration of them and your thoughts on how to proceed.

Sincerely,

W. E. Colby

DCI ltr to Admiral Anderson on Intelligence Leaks

Distribution:

Original - Addressee

- 1 - DCI
- 1 - DDCI
- 1 - ER
- 1 - C/PRD (& PRD Chrono)
- 1 - IC Registry
- 1 - PRD Subject
- 1 - PRD/OC
- 1 - [redacted] Chrono
- 1 - Chmn, SECOM

DCI/IC/PRD [redacted] 9 Sep 75)

STAT

STAT

STAT

Approved For Release 2004/05/12 : CIA-RDP80M01133A001100030002-2

Approved For Release 2004/05/12 : CIA-RDP80M01133A001100030002-2